National Aeronautics and Space Administration

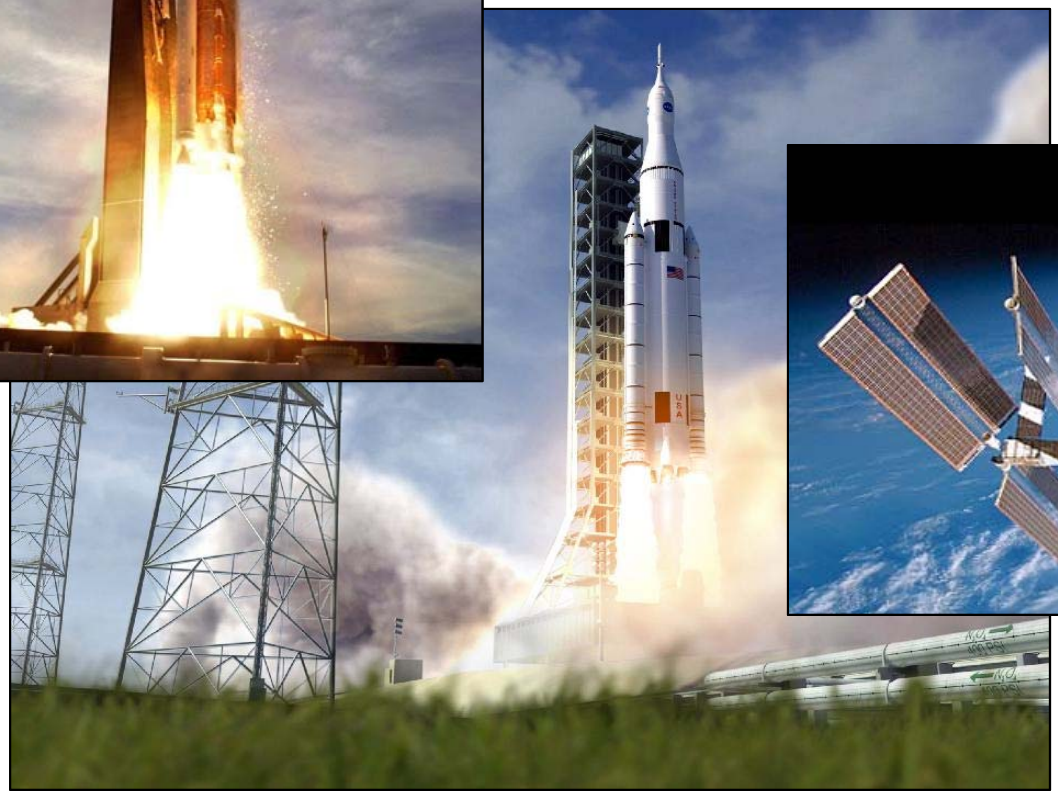
Space Systems Protection in a Cyber-Risk Environment

Jason A. Soloff
NASA Lyndon B. Johnson Space Center
Houston, TX

Presented at the University of Houston Clear Lake
Cyber Security Institute
Cyber Security Collaboration Forum
April 8, 2013

Topics

- NASA's position and exposure
- Cyber is "nothing new"
- Space viewed from a Cyber perspective
- The scope of NASA's challenge
- Systemic solutions



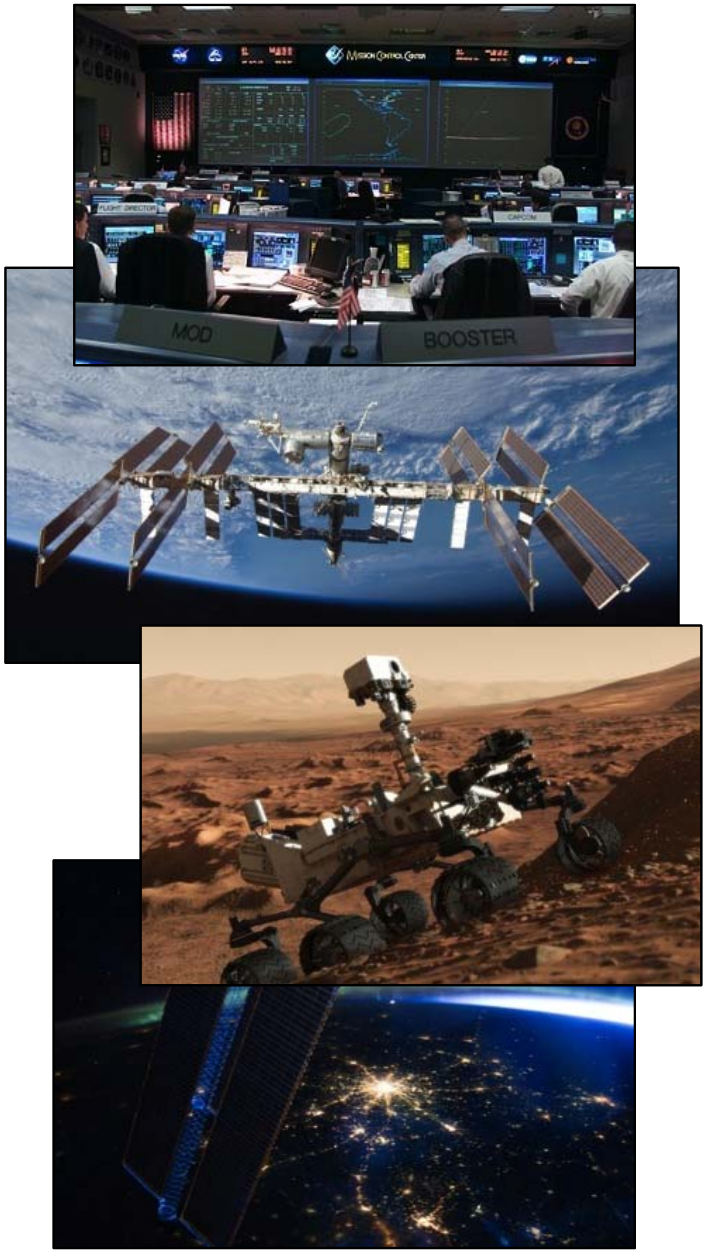
NASA as a symbol of National Excellence

- **Prestige** - NASA is seen by the world as a symbol of US economic, scientific and technical excellence and superiority.

- **Ideals** - NASA's missions, facilities and vehicles are visual representations of many of the United States' ideals and unique place as a champion of freedom and opportunity in the world.

- **Economic Power** – NASA's engineering and technology (along with NASA's commercial and academic partners) represent the produce of some of the best and brightest minds in the world – who have been working with significant national resources to back their research.

- NASA's accomplishments also draw **negative attention**
  - **Terrorism** – Attack in the most visible, publicly disturbing way possible.
  - **Espionage** – US technology is sought after by the rest of the world. US aerospace, computing and cutting-edge engineering is a vital resource that others want to capture and exploit.
  - **Suspicion** – Many nations (and non-state actors) view all US Government organizations as part of the US military or US intelligence community. This can lead them to see NASA as an extension of the military.



What the world thinks we do…

Aerospace Espionage in the “Bad Old Days”

Space
- Sys
- Ope
- Log
- 1st f

Buran
- Nea
- “De
- 1st (

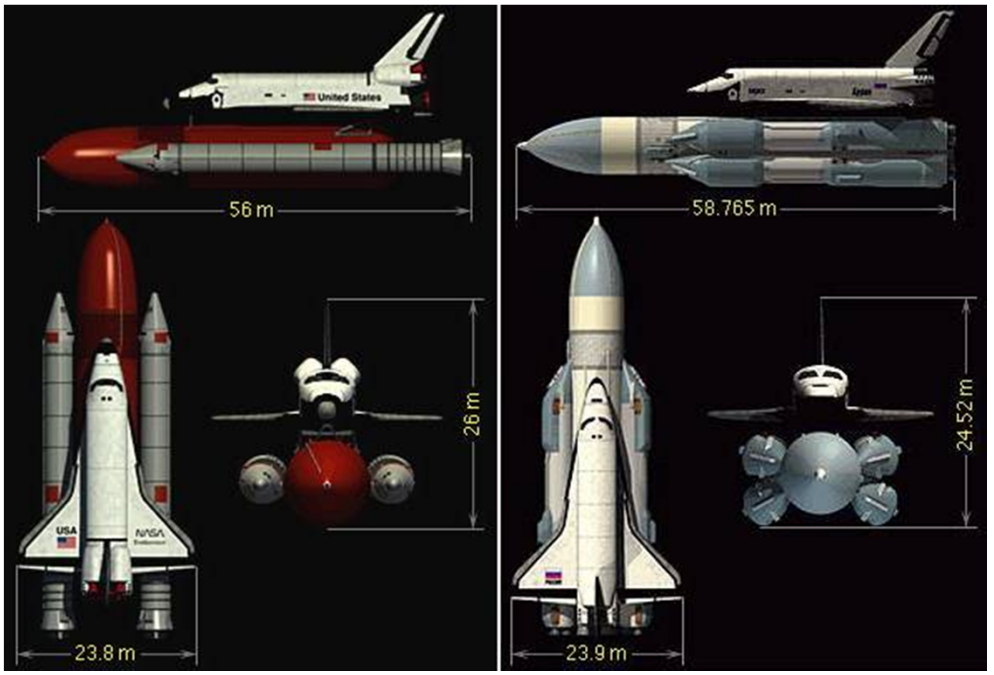
PATRIOTIC MISSION PATCHES

Chance? No, Cyber.

"When U.S. space shuttles started linking up with Russia's Mir space station in 1995, both sides owed a small debt to the old Soviet secret police, the KGB. **According to documents obtained by NBC News, it was the KGB that successfully stole the U.S. shuttle design in the '70s and '80s.**"

The key in terms of the shuttle program was "overt collection" and **specifically the use of commercial databases**. In effect, the massive effort directed at the U.S. space shuttle program was **among the first cases of Internet espionage**, if not the first case. With all the critical documents online, it was left to the VPK, under the auspices of the KGB, to gather it all up and then circulate it to those in the space program who needed it."

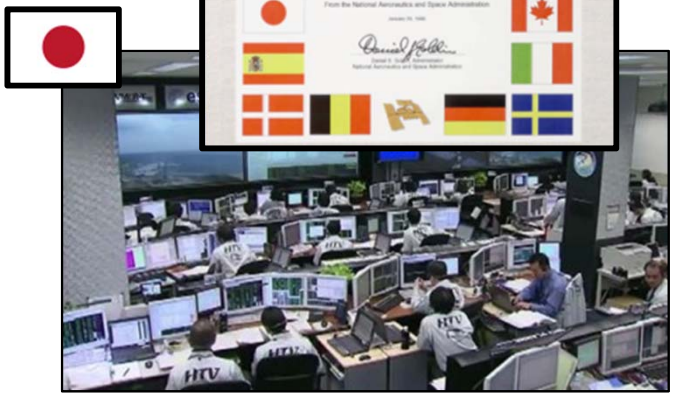
Source: "How the Soviets Stole a Space Shuttle", NBC News, Nov. 4, 1997



From the mid-1970s through the early 1980s, NASA documents and NASA-funded contractor studies **provided the Soviets with their most important source of unclassified material in the aerospace area.**
- CIA Analysis, 1985

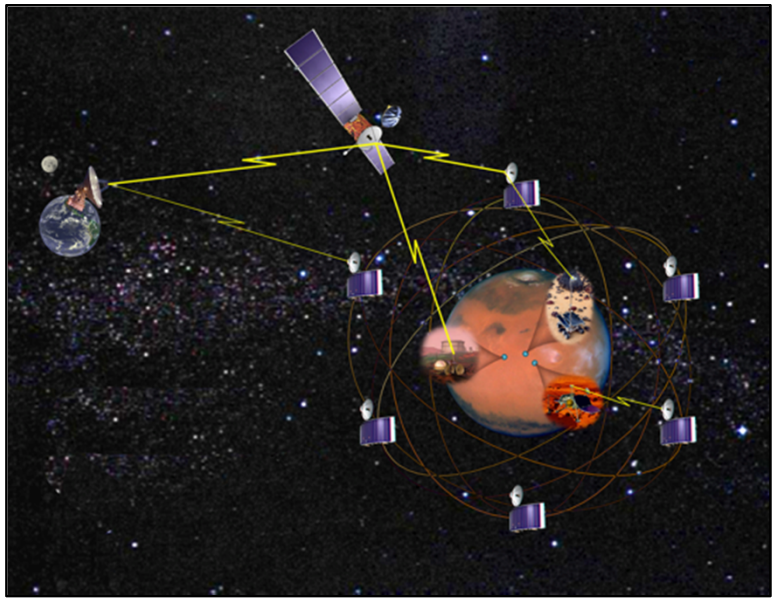
What HAS Changed?
The NASA Cyber Environment: Operations

- Today's space operations involves interconnection of multiple facilities, control centers, engineering organizations and science centers to accomplish the mission.
  - Many connections in and out of critical systems
  - Many organizations and individuals (students, foreign partners, commercial entities, other government agencies, etc.)
- Control infrastructure is (only) highly specialized applications and databases running on top of IT infrastructure.
- The challenge to cyber security in operations: NASA must do two (often opposed) things well:
  1. **Secure and protect the critical mission control / mission support infrastructure** and systems to ensure safe, successful mission operations, protection of sensitive data, and assured space flight capability.
  2. **Open up the critical mission control / mission support infrastructure** to partners, collaborators and the "public" to perform the science and outreach missions with which the Agency is chartered.



What HAS Changed?
The NASA Cyber Environment: Communications

- "Classic" space communications systems and architectures were very independent and stove-piped.
- Today's architectures are
  - Increasingly interconnected (multiple control centers, flight systems, ground stations)
  - Increasingly interoperable and shared (international partnerships)
  - Relying on modern network techniques and technologies to enable advanced mission concepts (eg. Mars Network)



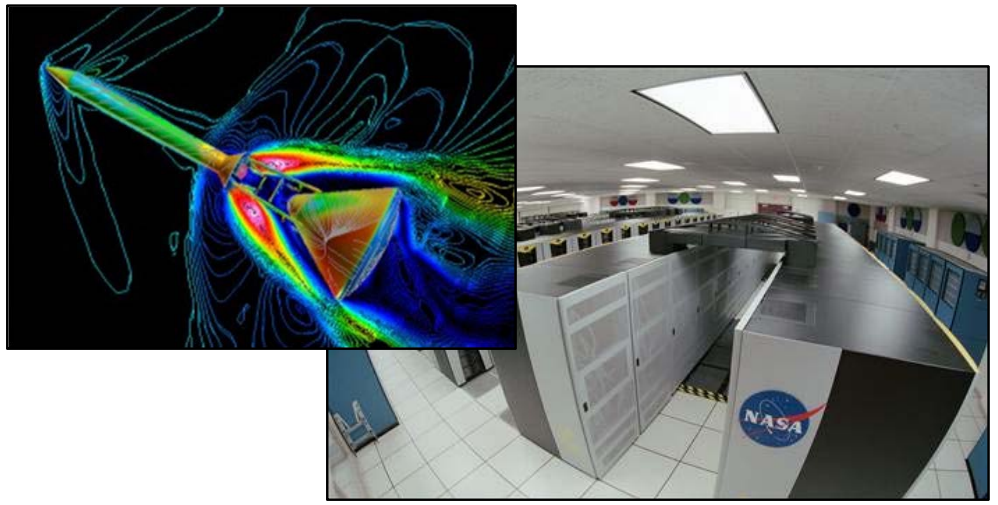
Massive improvements have also changed how we need to look at space communications in terms of assurance of communications:

- Confidentiality of the information
- Integrity of the information
- Availability of the capability to communicate

<u>Need to consider the effects of interconnectedness and the vulnerabilities that networked systems create.</u>

What HAS Changed?
The NASA Cyber Environment: Research / Engineering

- NASA's research and engineering represents some of the greatest investment made by the US in cutting edge technology.
- NASA research is conducted at
  - NASA Centers
  - Universities
  - NASA Contractor partners
  - NASA's international partners
- While NASA's data is not classified, it often contains highly sensitive and proprietary information that would certainly benefit companies and countries with less advanced technology, science and engineering ability.
- NASA's research and engineering
  - Databases and information repositories
  - Advanced modeling and simulation capabilities
  - Supercomputing (both capability and technology)



THE TOP THREE SUPERCOMPUTERS

SYSTEM	APPLICATIONS	BUILDER	ARCHITECTURE	PERFORMANCE (teraflops)	COST (US $, millions)
Blue Gene/L* Lawrence Livermore National Laboratory, Livermore, Calif.	Materials science, nuclear stockpile simulations	IBM	32 768 processors; 8 terabytes of memory; 28 terabytes of disk storage; Linux and custom operating system	70.72	100
Columbia NASA Ames Research Center, Moffett Field, Calif.	Aerospace engineering, simulation of space missions, climate research	SGI	10 240 processors; 20 terabytes of memory; 440 terabytes of disk storage; Linux operating system	51.87	50
Earth Simulator Earth Simulator Center, Yokohama, Japan	Atmospheric, oceanic, and earth sciences	NEC	5 120 processors; 10 terabytes of memory; 700 terabytes of disk storage; Unix-based operating system	35.86	350–500**

SOURCE: Top500 list (November 2004) and companies * Current configuration ** Industry estimate

What HAS Changed?
Organization – Separation of Mission and Institution

Programs & Mission Systems… Go Fly. Do the exploration. Bring back the science.

Mission Facilities (MCC, LCC)

Engineering (Labs/I&T)

Resident Program Offices / Teams

Institutional & Enterprise Services and Capabilities – Provide the foundation…

Security Services	IT Services	Physical Services	Business Operations
• Personnel Security • Perimeter (Physical) Security • Secure Network Capabilities	• Office Automation • IT Support • Information / IS Development and Hosting • Institutional IT Security	• Utilities • Buildings • Safety	• Logistics • HR/Payroll, etc. • Communications

The Threat to NASA (and US Aerospace) Today

- NASA's architectures are now incredibly intertwined and networked. **<u>It is no longer possible to accomplish NASA's mission using standalone communications and command / control architectures</u>**.
- **<u>Nation States</u>** take advantage of this
  - Motivated by national objectives
  - Economic / Military Advantage
  - Political / Diplomatic calculations
  - Cyber-espionage is a main aim
- **<u>Cyber-Terrorists</u>** take advantage of th
  - Politically motivated
  - Seek high degree of visibility
  - Aim is severe disruption
- **<u>Hacktivists</u>** take advantage of this
  - Motivated by "social consciousnes
  - Generally non-destructive
- **<u>Old School Hackers</u>** take advantage of this
  - Building "cred"
  - Hacking to test skills / for the challenge

… And NASA Has Been Hacked (Repeatedly)

"…NASA's status as a "target rich" environment for cyber attacks…"

"In 2010 and 2011, NASA reported 5,408 computer security incidents that resulted in the installation of malicious software on or unauthorized access to its systems. These incidents spanned a wide continuum from individuals testing their skill to break into NASA systems, to well-organized criminal enterprises hacking for profit, to intrusions that may have been sponsored by foreign intelligence services seeking to further their countries' objectives."

"these intrusions have affected thousands of NASA computers, caused significant disruption to mission operations, and resulted in the theft of export-controlled and otherwise sensitive data"

NASA Inspector General Paul Martin, Testimony before the US House of Representatives, February 29, 2012

Solutions NASA DOESN'T have…

So what solutions can NASA use?

Challenge Spaces:

1. NASA must look across Programs, Missions & Domains
2. Adversaries are looking at all avenues to get to targets
3. NASA's systems, programs and missions represent the "Crown Jewels" of the United States in terms of technology, national power and international prestige.
4. New programs = New technology = New "Targets"
5. Opening the "partner space" introduces huge opportunities …for both advancement and vulnerability

Solution Spaces:

1. Understand the Environment
2. Collaboration & Communities
3. Ensure rigorous processes and methods to produce information for decision makers.
4. Ensure common standards / training and language across practitioners.

Organizational Challenges to Addressing Cyber

NASA's culture

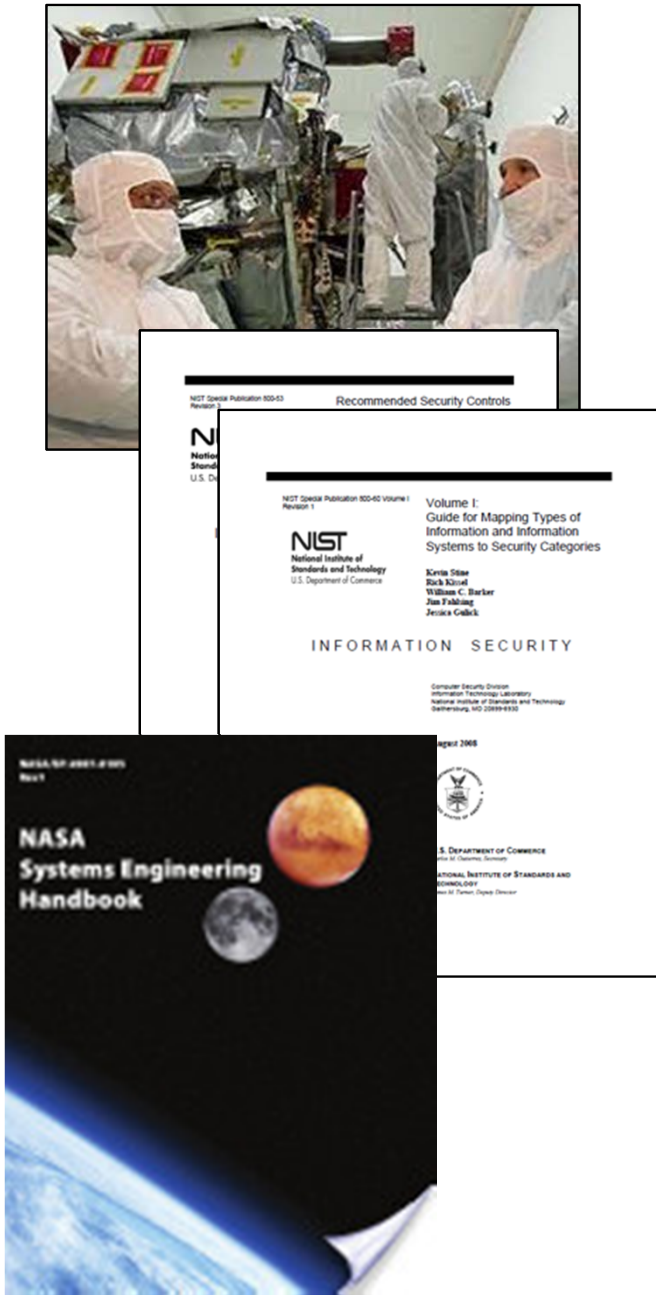
- "Failure is not an option."
- "We are an open, science organization…"
- "The world loves us!"
- "Mission" is separate from "Institutional"

NASA's mainstream experience base

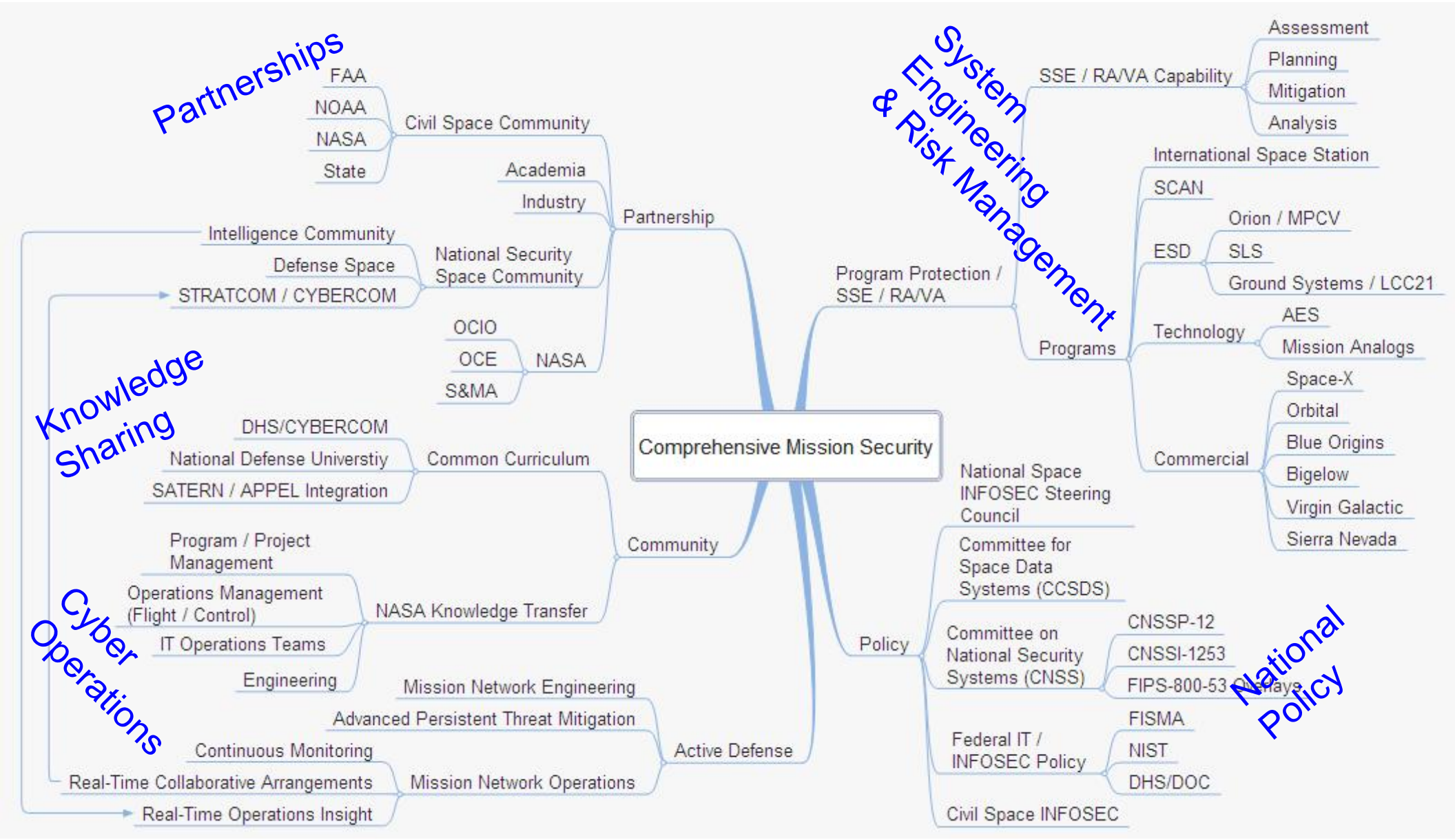
- Limited expertise in advanced networks (from an IT perspective)
- Very limited experience in malicious threat and harm mitigation
- An "IT centric" approach to Cyber fails to work in NASA's domain
  - It is not enough to "follow the FIPS or SANS playbooks". They simply don't marry well to the one-off space systems environment
- NASA's expertise is in systems engineering and mission operations which takes work to translate to Information Assurance

NASA's management approach

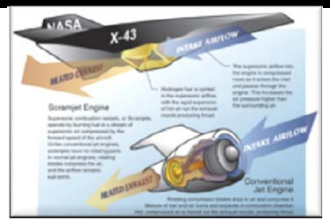
- Program management knobs: Cost, Schedule, Performance
- Security (Information Assurance, Counter-space) are "black arts"
  - A "security expert" participates in reviews and levies additional, unfunded requirements without explaining why
- Security is poorly understood as a technical engineering and operations discipline



The Scope
Requires Vertical and Horizontal Collaboration



How can we meet the challenge?
Communities. Capabilities. Practices.



Capability to Assess, Inform, Respond, and Protect Missions, Technology, Systems and Crew

Community of Practice

- Share Knowledge
- Develop Collaborative Relationships
- Cross-Train
- Bring together diverse discipline, experience and expertise.
- "None of us is as smart as all of us"

Analytical Capability

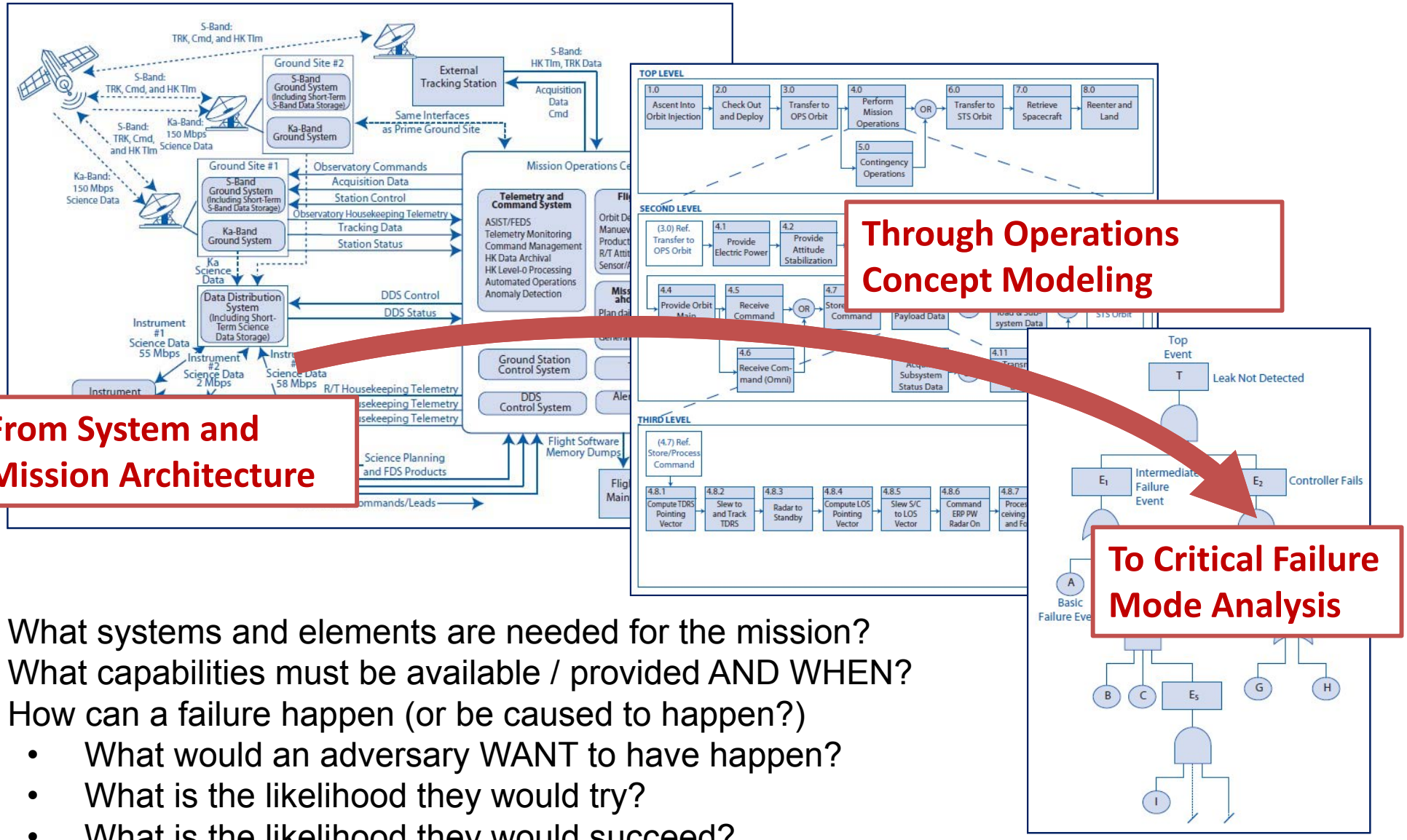
- Assess threats.
- Identify vulnerabilities.
- Identify risk.
- Evaluate mitigations.
- Provide insight to decision makers.

System (Security) Engineering Practices

- Provide methods and techniques to quantify.
- Leverage NASA system engineering discipline excellence to new domain.
- Provide rigor to ensure thorough identification, analysis and assessment.
- Leverage "best of breed" techniques for architecture analysis and assessment.

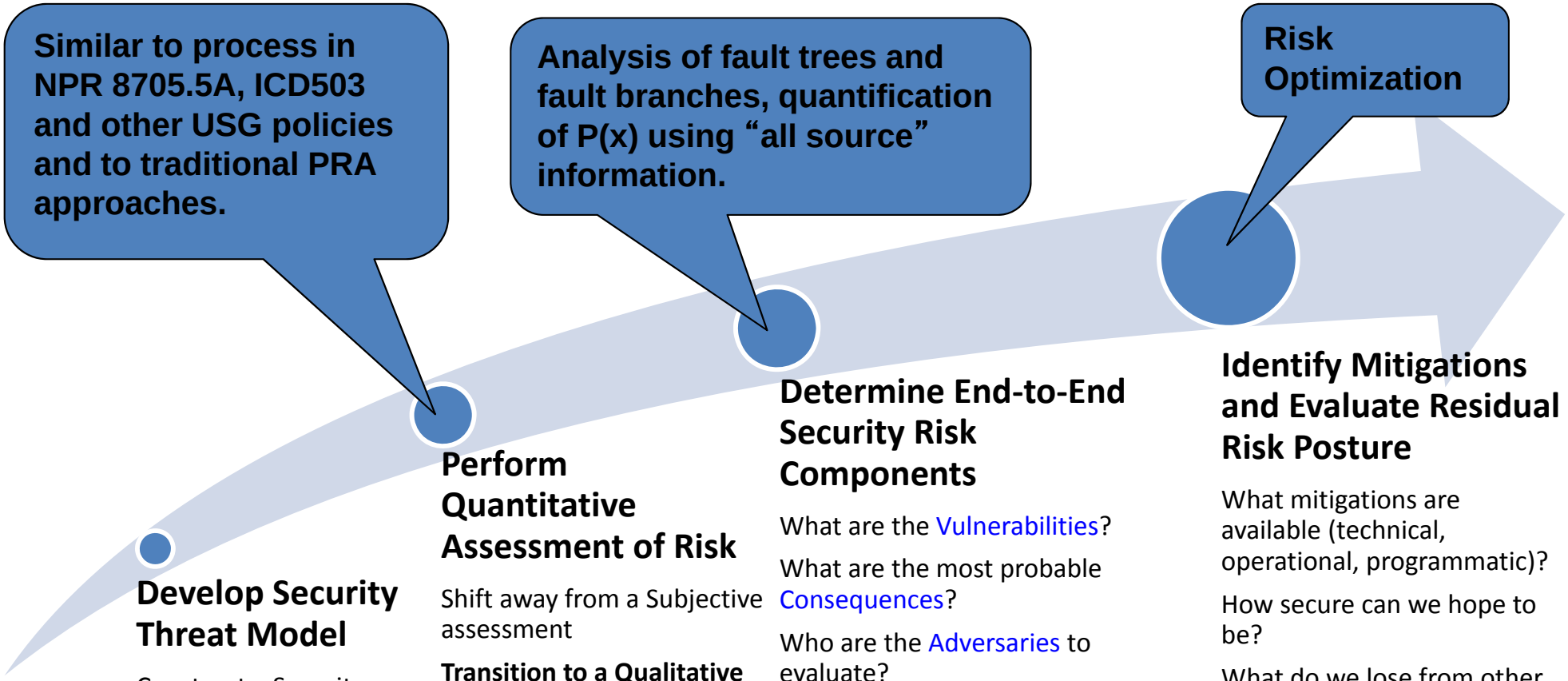
Collaborative Communication and Analysis Tools

Applying Rigor - System Security Engineering
Reconsidering how NASA does security risk management



1. What systems and elements are needed for the mission?
2. What capabilities must be available / provided AND WHEN?
3. How can a failure happen (or be caused to happen?)
   - What would an adversary WANT to have happen?
   - What is the likelihood they would try?
   - What is the likelihood they would succeed?

How do we measure how well we have engaged?
Security Risk Assessment Methodology



Develop Security Threat Model

Construct a Security Threat Model for the mission / system that **focuses solely on Intentional and willful efforts to attack and exploit**

Perform Quantitative Assessment of Risk

Shift away from a Subjective assessment

Transition to a Qualitative and then Quantitative approach.

Assess risk (i.e. Harm Value) as ranked to prioritized Consequence Values for the mission or system.

Determine End-to-End Security Risk Components

What are the Vulnerabilities?

What are the most probable Consequences?

Who are the Adversaries to evaluate?

What are the Harm Values (i.e. Assessed Risks) derived from the Probability of Success (by an Adversary(s)) standpoint?

Identify Mitigations and Evaluate Residual Risk Posture

What mitigations are available (technical, operational, programmatic)?

How secure can we hope to be?

What do we lose from other system goals? (cost / schedule / performance trade)?

When have we spent enough on security?

What is the remaining residual risk posture? Is it acceptable?

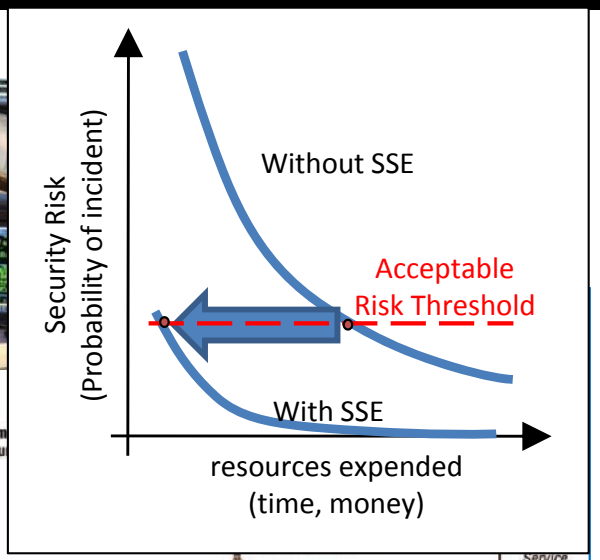
Tying it Together – The View Ahead

- Address integrated threat and risk mitigation activities throughout the life cycle of the project / program.
- Apply System Engineering rigor to the process of Security Risk management.
- Build and maintain strong Communities of Practice and use the collaboration and insight they provide.
- Iterative approach that constantly integrates new information and intelligence, refines the threat model, and evaluates emerging and evolving threat conditions against system and operations vulnerabilities.

Integrate stakeholders and experts to provide:

1. Quantitative risk / benefit information for use by key decision makers.
2. Quantitative analysis of threat and vulnerability to probable aggressor actions to inform operations to enhance safety, information protection and mission success.
3. Meaningful, actionable information across the community.

Sortie Crew and Cargo DRM



Contact Info

Jason A. Soloff
NASA Lyndon B. Johnson Space Center
Human Exploration Development Support Office (Code YI)
Houston, TX 77058

jason.a.soloff@nasa.gov
(281) 483-3554